## Math Background:

So before going into the diffie-hellman algorithm let's give some prerequisite math background

- **Fundamentals of Power:**
  - Product law → $x^a \cdot x^b = x^{ab}$
  - So we can use the product law in the opposite direction

$2 \mid a$ ⇒ This means a is divisble by 2

$$x^a = x^{a/2} \cdot x^{a/2}$$

$2 \nmid a$ ⇒ This means a is not divisble by 2, i.e. 'a' is odd

$$a = 1 + (a-1) \qquad 2 \mid a-1$$

$$x^a = x^1 \cdot x^{a-1}$$

$$= x \cdot x^{(a-1)/2} \cdot x^{(a-1)/2}$$

⇒ we can simply this by writing $x^a = x \cdot x^{\frac{a}{2}1} \cdot x^{\frac{a}{2}1}$

## • Fundamentals of Modular Arithmetic:

- First you Know

$a \% n = 0 \ldots n-1$

- Mod operator can be distributed smoothly among expressions

Addition: $(a+b) \% n = (a \% n + b \% n) \% n$

Multiplication: $(a b) \% n = (a \% n \cdot b \% n) \% n$

Proof: $(a+b) \% n = (a \% n + b \% n) \% n$

writing 'a' in terms of n

$a = qn + r$ q: quotient, r: remainder

e.g $a = 10$ $n = 3$

$10 = 3 \times 3 + 1$ $q = 3$, $r = 1$

Let's continue:

$a = q_1 n + r_1$ $b = q_2 n + r_2$

⇒ let's continue proofing ~~(a+b)%n~~

$$(a+b)\%n = (a\%n + b\%n)\%n$$

$$a = q_1 n + r_1 \quad b = q_2 n + r_2$$

$$(a+b)\%n = (q_1 n + r_1 + q_2 n + r_2)\%n$$

$$= [(q_1 + q_2)n + (r_1 + r_2)]\%n$$

Now we know that Mod removes all the cycles from a number, In other words

$$Kn\%n = 0 \quad \text{for } \forall K \in \mathbb{Z}$$

So $(q_1 + q_2)n \%n = 0$

So we can say

$$[(q_1 + q_2)n + r_1 + r_2]\%n =$$

$$(r_1 + r_2)\%n$$

So recall that Mod computes the remainder,

$$r1 = a\%n \quad r2 = b\%n$$

and that concludes our proof that

$$(a\%n + b\%n)\%n = (a+b)\%n$$

⇒ You can use the same principles to proof that for the case of Multiplication

$$(ab) \% n = (a \% n \cdot b \% n) \% n$$

- So we have talked a lot about Modular Arithmetic, now let's Combine Mod with Powers

$a^b \% n$ ~~We Know that~~

we know that $a^b = a^{b/2} \cdot a^{b/2}$ iff $2 \mid b$

, or $a^b = a \cdot a^{\lfloor b/2 \rfloor} \cdot a^{\lfloor b/2 \rfloor}$ iff $2 \nmid b$

So $a^b \% n = (a^{b/2} \cdot a^{b/2}) \% n$ iff $2 \mid b$

$= (a^{b/2} \% n \cdot a^{b/2} \% n) \% n$

That is a very very Imp Concept to understand about Mod with Powers

~~Fact 1: if we Know the Value~~ $a^{b/2} \% n$

~~Proof~~

⇒ Some facts about Mod and Power.

we have just shown that

$$a^b \% n = (a^{b/2} \% n \cdot a^{b/2} \% n) \% n$$

iff $2 \mid b$

AND

$$a^b \% n = (a \% n \cdot a^{\lfloor \frac{b}{2} \rfloor} \% n \cdot a^{\lfloor \frac{b}{2} \rfloor} \% n) \% n$$

iff $2 \nmid b$

Fact 1: We only need to Compute $a^{b/2} \% n$ to be able to know the value of $a^b \% n$

Fact 2: we can divide $a^{b/2} \% n$ further to $a^{b/4} \cdot a^{b/4}$

given the above 2 facts this implies that we can calculate

$a^b \% n$ in only $\log_2(b)$ steps

⇒ So $a^b \% n$ can be computed very efficiently even for very large values for the exponent

Bonus :

- Here is a pseudo code to show how $a^b \% n$ can be computed
- the following code is recursive

```
pow_mod(a, b, n) {
    if (b == 1) // base case
        return a%n;

    SubResult = pow_mod(a, |b/2|, n);
    SubResult = subResult * subResult;

    if (b%2 != 0) //odd exponent
        subResult = SubResult *
                    (a %n)

    return SubResult %n;
}
```